

AI Authorship Traceability Protocol (AATP)

Version 1.0

Date: February 24, 2026

Author: Frederick Redditt

Document Integrity Hash (Pre-Embed Reference):

265792fd62800b1b1d13fb5f3d25f1de330541b3a0c4fcf4fcd5cdd7c6380026

1. Purpose

The AI Authorship Traceability Protocol (AATP) establishes a minimal, platform-agnostic standard for preserving verifiable evidence of human intent and final artifact.

AI systems can obscure the visible link between human intent and final artifact. AATP restores that link through documented intent and cryptographic traceability.

This protocol is jurisdiction-neutral and tool-independent.

2. Core Principle

Authorship exists where verifiable human intent governs automated execution.

AI systems execute.

Humans author through intent, direction, selection, and accountability.

Traceability is the evidentiary bridge between intent and output.

3. Required Elements

3.1 Intent Record

A human must document the purpose, scope, and governing constraints of the work prior to or during generation.

3.2 Direction Record

Prompts, instructions, and material refinements that shape the output must be preserved.

3.3 Human Selection or Modification

A human must select, refine, or materially approve the final artifact.

3.4 Cryptographic Fingerprint

The final artifact must be hashed using SHA-256 or an equivalent collision-resistant cryptographic function.

3.5 Timestamp Anchoring

The hash must be anchored to a verifiable time source.

3.6 Chain Preservation

Intent record, direction record, final artifact, hash value, and timestamp reference must be archived together.

3.7 Reproducibility on Challenge

Upon dispute, the author must be able to present the preserved traceability chain:

Intent → Direction → Selection → Hash → Timestamp.

4. Platform Independence

AATP does not depend on any specific AI provider, jurisdiction, or platform policy.

5. Scope and Limitation

AATP establishes evidentiary traceability.

It does not automatically grant copyright or override jurisdictional law.

6. Cryptographic Anchoring Statement

This version embeds its pre-embed integrity hash above.

Any modification to this document will produce a different SHA-256 value.

The canonical hash of this final file must be independently verified and timestamp-anchored.